

20/5/17

مجموعات التوافقية " نظرية "

حالة أولي: دالة التوافقية

عبر هذه أولي: $a \in \mathbb{Z}$ $N \in \mathbb{N}$ $d(a, n) = 1$ حيث

$$\phi(n) = 1 \pmod{n}$$

الاشياء $(\mathbb{Z}_n, +, \cdot)$ حلقة

نمرقها الفرية تتألف

$$U(\mathbb{Z}_n) = \{ \bar{a} \in \mathbb{Z}_n : d(a, n) = 1 \}$$

اذا $d(a, n) = 1$ من العنصر $\bar{a} \in U(\mathbb{Z}_n)$ فلكي نرى هذه له فاني

و نسا لها فان $|G| = m$ $x \in G$ $x^m = e$ (الفاصل)

معنى هذا ان $\bar{a}^{-1} = \bar{a}^{\phi(n)}$ وحيث \bar{a} و \bar{a}^{-1} و \bar{a} و \bar{a}^{-1}

$$\bar{a}^{\phi(n)} \equiv 1 \pmod{n}$$

ننتج ان مجموعة من مالمات خاصة من اولي اذا كانت

$$d(p, a) = 1 \iff a^{p-1} \equiv 1 \pmod{p}$$

وحيث ان $\phi(p) = p-1$ وحيث ان

$$a^{p-1} \equiv 1 \pmod{p}$$

ننتج ان اذا كانت $n = p^k$ حيث ان p عدد اولي و k عدد صحيح

$$\phi(p^k) = p^k - p^{k-1}$$

ننتج ان اذا كانت الصيغة القانونية $p^k - p^{k-1}$ و $p^k - p^{k-1}$ فان

$$\phi(n) = n \prod_{p|n} (1 - \frac{1}{p})$$

الاشياء ϕ دالة متورية وحيث ان $p^k - p^{k-1}$ و $p^k - p^{k-1}$ و $p^k - p^{k-1}$

اولي متعلقة بغير اولي بكونه من $p^k - p^{k-1}$ و $p^k - p^{k-1}$

$$p^k - p^{k-1}$$

$$\begin{aligned}
 \phi(n) &= \phi(p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \dots p_k^{\alpha_k}) \\
 &= \phi(p_1^{\alpha_1}) \phi(p_2^{\alpha_2}) \dots \phi(p_k^{\alpha_k}) \\
 &= p_1^{\alpha_1} \left(1 - \frac{1}{p_1}\right) p_2^{\alpha_2} \left(1 - \frac{1}{p_2}\right) \dots p_k^{\alpha_k} \left(1 - \frac{1}{p_k}\right) \\
 &= p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right) \\
 &= n \cdot \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right)
 \end{aligned}$$

$\phi(360)$

نقل العدد إلى عوامله الأولية

$$360 \mid 2$$

$$180 \mid 2$$

$$90 \mid 2$$

$$45 \mid 3$$

$$15 \mid 3$$

$$5 \mid 5$$

$$360 = 2^3 \cdot 3^2 \cdot 5$$

$$\phi(360) = 360 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right)$$

$$= 360 \left(\frac{1}{2}\right) \left(\frac{2}{3}\right) \left(\frac{4}{5}\right)$$

$$= 360 \frac{4}{15} = 96$$

أي

$$|U(\mathbb{Z}_{360})| = 96$$

$$U(\mathbb{Z}_{360}) = \{a \in \mathbb{Z} \mid (a, 360) = 1\}$$

مثال

$$3^{256}$$

نصف العناصر السالبة
العديدين الأساسيين للعدد

العدد الطول هو 256 وهذا العدد على 100

$$3^{256} \equiv x \pmod{100}$$

وهذا العدد

نقد خط آخر $d(3, 100)$ اولیات مفید می باشد. عدد اول

$$\phi(100) \equiv 1 \pmod{100}$$

علی‌هذا نسبت $\phi(100)$ و عدد 256 که معادل
صند است 100

$$\phi(100) = \phi(2^2 \cdot 5^2) = 100 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) \\ = 100 \left(\frac{1}{2}\right) \left(\frac{4}{5}\right) = 40 = \boxed{40}$$

اذا كانت n اكرت الفاس فاعلم ان n مع

$$256 = 6 \cdot 40 + 16$$

$$\frac{256}{3} = \left(\frac{40}{3}\right)^6 \cdot 3^6 = 1^6 \cdot 3^6 \pmod{100}$$

$$\frac{256}{3} \equiv 3^6 \pmod{100} \\ \equiv (-19)^4 \pmod{100} \equiv (-19)^2 \pmod{100}$$

$$\equiv (1-19)^2 \pmod{100}$$

$$\equiv (361)^2 \pmod{100}$$

$$\equiv (61)^2 \pmod{100}$$

$$\equiv (-39)^2 \pmod{100}$$

$$\equiv 1521 \pmod{100}$$

$$\equiv (15 \cdot 100 + 21) \pmod{100} \\ \equiv 21 \pmod{100}$$

$$\boxed{(563)^{256} = (256)^3 \pmod{100}} \quad \text{اذا كانت n اكرت الفاس فاعلم ان n مع}$$

إثبات أن الأسس أكبر من المقاس استنبطه بالبرهان
 ثم إن قيمة المقادير مع دالة أولية
 لفرقتان $n, m \in \mathbb{Z}^+$ حيث أن
 $d(n, m) = 1$ أوليات متباينتين

$$[m^{\phi(n)} + n^{\phi(m)}] \equiv 1 \pmod{nm}$$

من أجل إثبات أن $d(n, m) = 1$

$$m^{\phi(n)} \equiv 1 \pmod{n} \Rightarrow m^{\phi(n)} - 1$$

$$n^{\phi(m)} \equiv 1 \pmod{m} \Rightarrow m^{\phi(m)} - 1$$

حيث n, m أوليات فإن n, m يقسم عدد فردي

$$n, m \mid (m^{\phi(n)} - 1)(n^{\phi(m)} - 1)$$

$$n, m \mid [m^{\phi(n)} n^{\phi(m)} - m^{\phi(n)} - n^{\phi(m)} + 1]$$

وأيضا $n, m \mid m^{\phi(n)} - 1$ و $n, m \mid n^{\phi(m)} - 1$

وبذلك لدينا $n, m \mid [a]$ و $n, m \mid c$

$$b \mid n, m \text{ والآن نأخذ بقسم القسمة}$$

$$n, m \mid (n^{\phi(m)} + n^{\phi(n)} - 1)$$

$$n^{\phi(m)} + n^{\phi(n)} \equiv 1 \pmod{n, m}$$

حيث أن $\phi(n)$ هو عدد زوحي فلها n حوصاً
 لفرقتان n كتب على شكل عدد أولي

$$n = p_1^{v_1} \cdot p_2^{v_2} \cdots p_k^{v_k} \quad \text{أي الصيغة القياسية}$$

$$\phi(n) = p_1^{v_1-1} \cdot p_2^{v_2-1} \cdots p_k^{v_k-1} (p_1-1)(p_2-1) \cdots (p_k-1)$$

$$\frac{n}{\prod (p_i-1)}$$

$$p_1 \cdot p_2 \cdots p_k \quad \text{صحيح لأن } p_i \text{ أولية مميزة}$$

افضل من 2 و... والناتج سيكون العدد الذي

$$k \geq 2 \quad n = 2^k \quad \text{إذا كان من الشكل}$$

$$\phi(2^k) = 2^k - 2^{k-1} = 2^{k-1} (2-1) = 2^{k-1}$$

نوهي

(ب) إذا كان ليس من الشكل السابق أي (ن لم يكن قوة للعدد 2) فهو يقبل الصيغة مع عدد أولي أولي p أي

$$n = p^s \cdot m \quad s \geq 1$$

ولم يكن صيغة $d(p, m)$ هي $d(p^s, m)$ و ϕ ذات

$$\phi(n) = \phi(p^s) \cdot \phi(m)$$

$$= \phi(m) \cdot p^{s-1} (p-1)$$

نفس النظر

مع القدر $p^{s-1} \cdot \phi(m)$ كما في $\phi(n)$ مما سبق

نكتب نوهي

$$22 // \left(\frac{10n+2}{3} + 5 \right) \cdot 2 \quad \text{نقسم (22) بقسمة 2}$$

لأنه

$$22 = 2 \cdot 11 \quad (10)^n \cdot 3^2$$

(ج)

وناف

$$d(3, 22) = 1$$

$$3^5 \equiv 1 \pmod{22} \quad \text{عدد أولي نسبي}$$

$$5^5 \equiv 1 \pmod{22} \quad \text{عدد أولي نسبي}$$

$$\phi(22) = 2 \cdot 11 = \phi(2) \cdot \phi(11) = 1 \cdot 10 = 10$$

$$3^{10} \equiv 1 \pmod{22} \quad 5^{10} \equiv 1 \pmod{22}$$

$$= \left[3^{10n+2} + 5^{10n+3} - 2 \right] \cdot 2 \left[(3^{10})^n \cdot 3^2 + (5^{10})^n \cdot 5^3 - 1 \right]$$

$$= ((1)^n \cdot 3^2 + (1)^n \cdot 5^3 - 2) \pmod{22}$$

$$= (132) \pmod{22}$$

$$22 \text{ mod العدد}$$

وبالتالي فإن

نقسم العدد

$$\equiv 0 \pmod{22}$$

نقسم العدد n أولي إذا وفقط إذا كان $n-1$ $\phi(n)$

إذا كان n أولي فإن $n-1$ $\phi(n)$ لأن جميع الأعداد أصغر من n أولي

$n-1$

نقسم العدد n أولي إذا وفقط إذا كان n أولي

لأن n أولي إذا كان n مغلفا لعدد قاسم لمثل d

$1 < d < n$: $d \mid n$ أي يوجد بين مجموع الأعداد

$1, 2, 3, \dots, n-1$ عدد واحد من الأعداد

لنعتبر أولاً مع n وعندئذ سوف يكون $n-2 \leq \phi(n)$ وهذا يتناقض مع فرضنا $\phi(n) \leq n-1$ ولذلك n لا يمكن أن يكون غير أولي.
 أي n أولي.

تمرين: نثبت أن n عدد صحيح موجب $\phi(n)$ عند

1- إذا كان n فردية فإن $\phi(2n) = \phi(n)$

2- n زوجية فإن $\phi(2n) = 2\phi(n)$

الحل: إذا كان n فردية فإن $d(2, n) = 1$ $\phi(2, n) = \phi(2) \cdot \phi(n) = 1 \cdot \phi(n) = \phi(n)$

و $\phi(2, n) = \phi(2) \cdot \phi(n) = 1 \cdot \phi(n) = \phi(n)$

2- $n = 2^k \cdot m$; $d(2^k, m) = 1$
 $\phi(n) = \phi(2^k \cdot m) = \phi(2^k) \cdot \phi(m) = 2^{k-1} \cdot \phi(m)$

$\phi(2n) = \phi(2 \cdot 2^{k-1} \cdot m) = \phi(2^k \cdot m) = 2^{k-1} \cdot \phi(m)$

$\phi(2n) = 2 \cdot 2^{k-1} \cdot \phi(m) = 2 \cdot \phi(n)$

$\phi(2n) = 2 \cdot \phi(n)$

$\phi(2n) = 2 \cdot \phi(n)$

$\phi(2n) = 2 \cdot \phi(n)$

$\phi(2n) = 2 \cdot \phi(n)$

$\phi(2n) = 2 \cdot \phi(n)$

$\phi(2n) = 2 \cdot \phi(n)$

$\phi(2n) = 2 \cdot \phi(n)$

$\phi(2n) = 2 \cdot \phi(n)$

$\phi(2n) = 2 \cdot \phi(n)$

$\phi(2n) = 2 \cdot \phi(n)$

$\phi(2n) = 2 \cdot \phi(n)$

والثاني إذا أخذت d جميع مقاسم n متنا d تقع أيضا
 جميع المقاسم حيث $\sum_{d|n} \phi(d)$ تاربي

$$\sum_{d|n} \phi(d) = \sum_{\substack{d|n \\ d \neq 1}} \phi\left(\frac{n}{d}\right)$$

جميع المقاسم n $d \in \{1, 2, 3, 4, 6\}$
 والمقام القاسم لها $\frac{n}{d} \in \{12, 6, 4, 3, 2, 1\}$

ملاحظة: $1 \leq n$ عدد طبيعي فإن

$$n = \sum_{d|n} \phi(d) = \sum_{\substack{d|n \\ d \neq 1}} \phi\left(\frac{n}{d}\right)$$

مجموع مقاسم العدد n والآخر $d|n$
 تاربي درجاً العدد n .

الصفات: انوع العدد n $1, 2, 3, 4, \dots, n$
 هي صفوف على الترتيب إذا كان

$$d|n \quad S_d = \{m \mid d(m, n) = d\}, 1 \leq m \leq n$$

فمثلاً $S_3 = \{15\}$

أي أن S_d تآلت رؤسها لعل من العدد n
 التي هي أصغر أو تاربي m وأكبر تاربي 1
 وفي القاسم المبرر في هذه العدد d تاربي d

أي أن عدد $\phi(n)$ $\{1, 2, 3, 4, 6, 12, 15\}$
 وكانت إذا كان $d \mid d(m, n) = d$ هذه الصفوف

صفت أن يوجد m, n $n \mid m, m \mid n$
 $n = n_0 \cdot d$
 $m = m_0 \cdot d$
 صفت أن يوجد m, n $n \mid m, m \mid n$

ونقار كل قيمة m قيمة واحدة ل m دمية واحدة ل d لنا
 فإن عدد عناصر كل مجموعة S_d ~~تساوي~~ عدد الأعداد m
 أن $m = m$ والأولية ل n مع n وهذا n والتي لا تتغير
 n أن d عدد عناصر S_d يساوي عدد الأعداد الأولية
 التي لا تتجاوز n والأولية معها أي $\phi(n)$ يساوي
 $\phi(n)$ أن d أن n

ولمّا أن كل من الأعداد في هذه المجموعة يقسم n فمقتضى
 واحد من S_d بهذا $\phi(n) \leq n$ هو $\phi(d)$ N/n

مثال $n = 10$ فمجموع n هي $\{1, 2, 5, 10\}$ ولنفرض المجموعة S_d
 $S_1 = \{m; d(m, 10) = 1; 1 \leq m \leq 10\}$
 $m = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10$

$S_1 = \{1, 3, 7, 9\}$ الأولية = 4

$d(m, 10) = 2$

$S_2 = \{2, 4, 6, 8\}$

$d(m, 10) = 5$

$S_5 = \{5\}$

$S_{10} = \{10\}$

• $|S_1| = 4 \Rightarrow \phi(n) = \phi(10) = \phi(10) = 4$

• $|S_2| = 4 \Rightarrow \phi(10) = \phi(5) = 4$

• $|S_5| = 1 \Rightarrow \phi(10) = \phi(2) = 1$

• $|S_{10}| = 2 \Rightarrow \phi(10) = \phi(1) = 1$

$$\phi(1) + \phi(2) + \phi(5) + \phi(10) =$$

$$1 + 1 + 4 + 4 = 10$$

وذلك يكون

الدالة ϕ - ٢

تسمى الدالة ϕ (تأري) وهي دالة هامة فيتمتعها عدد

$$\phi(n) = \text{عدد القواسم الموجبة المختلفة للعدد } n$$

$$\phi(3) = 2 \quad \phi(4) = 3 \quad \phi(5) = 2$$

قواسم 4 هي 1, 2, 4

$$\phi(10) = 4 \quad \text{قواسمها هي } 1, 2, 5, 10$$

$$\phi(p) = 2 \quad \text{أولي } p$$

قواسم العدد p هي 1, p

يرتبط الدالة ϕ هذه الدالة هامة

للدالة ϕ يمكن اشتقاق الدالة ϕ

$$\phi(n) = \sum_{d|n} \phi(d)$$

الدالة ϕ هي الدالة $\phi(d)$ إذا $d|n$ دالة هامة تماماً

$$\phi(d, d) = 1 \quad \phi(n) = 1$$

$$\phi(d, 1) = \phi(1) = 1$$

يمكن تعميمها إذا كانت ϕ دالة هامة فإن الدالة المعروفة

تلك المعروفة $\phi(d)$ $\phi(n) = \sum_{d|n} \phi(d)$ يمكن تعميمها أيضاً

$$\phi(n) = \sum_{d|n} \phi(d)$$

مثال الحالة 3

① $n = p^{\alpha}$ p أولي $\alpha \geq 1$ فان قواسم n العنصرية هي
 $1, p, p^2, \dots, p^{\alpha-1}, p^{\alpha}$

مما يجعل عددها $\alpha + 1$ اي

$$\tau(p^{\alpha}) = \alpha + 1$$

② الصيغة القاسمية لـ n هي

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1)$$

بما ان $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} \subset p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ اولية

$$\tau(n) = \tau(p_1^{\alpha_1}) \dots \tau(p_k^{\alpha_k})$$

$$= (\alpha_1 + 1) \dots (\alpha_k + 1)$$

$$\tau(n) = \prod_{i=1}^k (\alpha_i + 1)$$

مثال

$$\tau(63) = \tau(3^2 \cdot 7^1)$$

$$(\alpha_1 + 1)(\alpha_2 + 1) = (2 + 1)(1 + 1) = 6$$

- قواسم 63 : $1, 3, 7, 9, 21, 63$ عددها هو 6

حالة 4

تعريف: هي حالة ماسية تقابل العدد الصحيح الموصي

n مجموع القواسم العنصرية للعدد n

$$\sigma(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28$$

مثلا

$$\tau(12) = 6$$

قواسم 12 : $1, 2, 3, 4, 6, 12$

$$\tau(2^2 \cdot 3^1)$$

$$(2 + 1)(1 + 1) = 3 \cdot 2 = 6$$

$$\sigma(1) = 1 \quad \sigma(2) = 3 \quad \sigma(3) = 4$$

$$\sigma(4) = 1 + 2 + 3 + 4 = 7$$

$$\sigma(p) = 1 + p \quad \tau(p) = 2$$

$$\sigma(n) = \sum_{d|n} d \quad \text{وذلك الشكل}$$

$$d|n \Rightarrow \sum_{d|n} f(d) \quad ; \quad f(d) = d$$

هذه هي الدالة التي تعرف بالعدد d في $f(d)$ هي القيمة
 متماثلًا لأن $f(d_1 d_2) = f(d_1) f(d_2)$
 $d_1, d_2 = f(d_1) f(d_2)$

والدالة العددية هي التواليف $\sum_{d|n} f(d)$

حالات الخاصة σ

$$1, p, p^2, \dots, p^{n-1}, p^n \quad n = p^n$$

$$\sigma(n) = 1 + p + p^2 + \dots + p^{n-1} + p^n$$

هي عبارة متسلسلة هندسية وهذا الشكل هو
 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100

$$\sigma(n) = \frac{1 - p^{n+1}}{1 - p}$$

العبارة القانونية لـ σ

$$\sigma(n) = \prod_{i=1}^k \frac{p_i^{a_i+1} - 1}{p_i - 1}$$

نموذج σ للدور τ والدور

بـقـة مـا صـيـر قـطـريـة الـزحـاد

الانبات $P_1^{a_1} \dots P_k^{a_k}$ اوليت من حيث

$$\sigma(n) = \sigma(P_1^{a_1}) \dots \sigma(P_k^{a_k})$$

$$= \frac{P_1^{a_1+1} - 1}{P_1 - 1} \cdot P_2$$

اذا كان P عدد اولي

$$\sigma(P) = \frac{P^2 - 1}{P - 1} = (P-1)(P+1) = \boxed{P+1}$$

مثال: $\sigma(180)$ $\sigma(180)$ ام

$$180 = 2^2 \cdot 3^2 \cdot 5$$

$$90 = 2 \cdot \sigma(180) = \sigma(2^2 \cdot 3^2 \cdot 5)$$

$$45 = 3 \cdot$$

$$15 = 3 \cdot \frac{2^3 - 1}{2 - 1} \cdot \frac{3^3 - 1}{3 - 1} \cdot \frac{5^2 - 1}{5 - 1}$$

$$5 = 5 \cdot 2 - 1 \quad 3 - 1 \quad 5 - 1$$

$$1 = 7 \cdot 13 \cdot 6 = 546$$

$$\sigma(180) = \sigma(2^2 \cdot 3^2 \cdot 5)$$

$$(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1) = (2+1)(3+1)(1+1)$$

$$= 18$$

ملحوظة: ان الدالة σ ليست اقليدية

$$\sigma(20) = \sigma(2 \cdot 10)$$

صحة خطأ

$$\sigma(2) \cdot \sigma(10)$$

مركبات

صحة خطأ

$$2 \cdot 4 = 8$$

$$\tau(20) = (2^2 \cdot 5) = 6$$

$$\tau(2^2 \cdot 5) \neq \tau(2 \cdot 10)$$

وهذه ليست خلية تماماً

$$\sigma(20) = \sigma(2^2 \cdot 5) = \frac{2^3-1}{1} \cdot \frac{5^2-1}{5-1} = 7 \cdot 6 = 42$$

$$\sigma(2) \cdot \sigma(10) = 3 \cdot (1+2+5+10)$$

$$3 \cdot 18 = 54$$

$$\sigma(2^2 \cdot 5) \neq \sigma(2) \sigma(10)$$

وبالتالي ليست خلية تماماً

نقطة انتبه ان هذا رقم القواسم الجوهرية للعدد n سيأتي

$$\tau(n) = (n)^{\frac{1}{2}} = \sqrt{n \tau(n)}$$

$$d/n \Leftrightarrow d/n \quad \text{الضاب}$$

$$n = d \cdot d'$$

ولمّا كان عدد القواسم الجوهرية لـ n يساوي $\tau(n)$

وحيث $n = 10$ وبما أن n ليس عدداً مربعاً كاملاً

$$n = 10 \quad \tau(n) = 4 \quad \text{يساوي} \quad d \cdot d' \quad \begin{matrix} 1 & 2 & 5 & 10 \end{matrix}$$

وعند ضرب هذه العلاقات نحصل على

$$(n)^{\tau(n)} = \prod_{d|n} d \cdot \prod_{d'|n} d'$$

إذاً انتبه d جميع قواسم n هنا

d مع n/d جميع قواسم n هنا

$$\prod_{d|n} d = \prod_{d'|n} d'$$

$$10 \cdot 2 \cdot 1 \cdot 10$$

$$= 2 \cdot 5$$

$$= 10 \cdot 1$$

$$= 5 \cdot 2$$

$$\tau(n) = \left(\prod_{d|n} d \right)^2 \rightarrow \text{والتالي فان}$$

$$\prod_{d|n} d = \sqrt{n \tau(n)}$$

$$\frac{\sigma(n)}{n} = \sum_{d|n} \frac{1}{d} \quad \text{نقريته}$$

$$\text{أو } \sigma(n) = n \cdot \sum_{d|n} \frac{1}{d}$$

$$\sigma(n) = \sum_{d|n} d = \sum_{d|n} \frac{n}{d} \quad \text{الذاتية: نلاحظ بالقرينة أن}$$

ولكنه فهو قد قسم n بالعدد d في

d_1, d_2, \dots, d_k فنتيجة

$$\sigma(n) = \frac{n}{d_1} + \frac{n}{d_2} + \dots + \frac{n}{d_k}$$

$$= n \cdot \left(\frac{1}{d_1} + \frac{1}{d_2} + \dots + \frac{1}{d_k} \right)$$

$$\sigma(n) = n \sum_{d|n} \frac{1}{d} \quad \text{أو عدد العدد n في}$$

n الذي يحذف العلامة التالية

$$\sigma(10) = 10$$

$10 = 2 \cdot 5$ هو عدد عددين أوليين لذلك

$10n$ ليس أن يكون من الشكل

$$10 \cdot n = 2^a + 5^b$$

نقريته

سؤال
المتن

المتن

وعندما يكون 2^{25} $\gamma(10n) = (\alpha+1)(\beta+1)$ $\alpha+1=2$ $\beta+1=5$ $\Rightarrow \alpha=1$ $\beta=4$

$$\alpha+1=2 \quad \beta+1=5 \quad \Rightarrow \quad \alpha=1 \quad \beta=4$$

$$\Rightarrow 10n = 2^1 \cdot 5^4 \Rightarrow n \cdot 2 \cdot 5^3 = \boxed{125}$$

$$\alpha+1=5 \Rightarrow \alpha=4$$

$$\beta+1=2 \Rightarrow \beta=1$$

$$10n = 2^4 \cdot 5^1 \Rightarrow \boxed{n=8}$$

تعريف: نقول عن العدد الصحيح انه كامل اذا كان

$$\sigma(n) = 2n$$

أصغر عددين تامين كاملين معرطين $n=6$ $n=28$

$$\sigma(6) = 12 = 2 \cdot 6$$

يقال عن العدد n كامل اذا كان $\sigma(n)$ اكبر منه

يقال ان العددين m, n متكاملين متتامين اذا كان

$$\sigma(m) = \sigma(n) = m+n$$

ان العددين 220 284 ~~248~~ عددين متتامين

ملحظة: اوجد العلماء عددين الاعداد التي حاصلتها

نوعيه وهما الان شقت السائل معمولة في كتاب

خروجي

نسبة الاعداد في الشكل $1 - \frac{1}{2^k} = \frac{1}{2^k}$ $k \geq 2$

الاعداد غير نسبية وتسمى الاعداد المنزلية في الشكل $1 - \frac{1}{2^k}$

او لثابت غير نسبية

تعريف دالة موبس:

n عدد صحيح طبيعي الشكل التالي:

$$\mu(n) = \begin{cases} 1 & ; n=1 \\ 0 & ; p^2 | n \text{ عدداً كلاً} \\ (-1)^r & ; n = p_1 \cdot p_2 \cdot \dots \cdot p_r \end{cases}$$

$$\mu(30) = 2 \cdot 3 \cdot 5 = (-1)^3 = -1$$

مثال

$$\mu(10) = \mu(2 \cdot 5) = (-1)^2$$

$$\mu(12) = \mu(2^2 \cdot 3) = 0$$

وبرسعت أن دالة موبس دالة مضروب

دالة ليوفليك: تعرفت على النمو التالي

$$\lambda(n) = \begin{cases} 1 & ; n=1 \\ (-1)^{\alpha_1 + \alpha_2 + \dots + \alpha_r} & ; n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_r^{\alpha_r} \end{cases}$$

المرتبة الأخرى: الكثرة الزولية والدولة

المركبة: ان رتبة a المقاس m أو الأسس التي
 ينقسم اليها a بالمقاس m حيث $a \in \mathbb{Z}$ $d(a, m)$ هو
 اصغر عدد صحيح موجب k موزع لاساوي بالعنصر بحيث الشرط
 $a^k \equiv 1 \pmod{m}$

ويقال عن k هو بديل أولي (دليل للعنصر المقاس)
 $(m, a) = 1$ حيث $k = \sum d/a$
 $= \sum d/a \pmod{m}$

مثال: ما هي مرتبة 2 بالمقاس 7

$$2^2 \equiv 4 \pmod{7}$$

$$2^3 \equiv 1 \pmod{7}$$

أي مرتبة 2 بالمقاس 7 هي 3

$$\text{ord } 2 = 3$$

7

$$\text{ord } 5 = 2 \quad 5^2 \equiv 1 \pmod{6}$$

6

$$\text{ord } 3 =$$

14

$$3^2 \equiv 9 \pmod{14}$$

$$3^3 \equiv 13 \pmod{14}$$

$$3^4 \equiv 11 \pmod{14}$$

$$3^5 \equiv 1 \pmod{14}$$

$$14 \sqrt{81}$$

$$3^6 = 1 \pmod{14}$$

سيفي

$$\text{ord } 3 = 6$$

مبرهنة: إذا كان رتبة العدد الصحيح a المقاس m تساوي 14

$$a^S \equiv 1 \pmod{m} \quad \text{فإن} \quad K | S$$

على العكس، إذا كان $K | S$ فإن $S = k_1 \cdot k_2$ ومنه

$$a^S = (a^{k_1})^{k_2} \equiv (1)^{k_2} \pmod{m} \equiv 1 \pmod{m}$$

إذا كان S عدد صحيح حقيقى

$$a^S \equiv 1 \pmod{m}$$

الصفة $S = q \cdot K + r \quad 0 \leq r < K$

$$a^S = (a^K)^q \cdot a^r \equiv 1 \pmod{m}$$

$$a^r \equiv 1 \pmod{m}$$

وبسبب تعريف الرتبة فإن K أصغر عدد صحيح موجب يحقق الصفة

$$a^S \equiv 1 \pmod{m} \quad \leftarrow S = q \cdot K + r$$

↑

نفسه إذا كان K رتبة a المقاس m فإن $K | \phi(m)$

لأنه من مبرهنة أويلر $a^{\phi(m)} \equiv 1 \pmod{m}$ نظايت a مع m حيث

$$a^{\phi(m)} \equiv 1 \pmod{m} \quad \text{إذا كان } K \mid \phi(m)$$

ومن ثم لا بد من أن K يقسم $\phi(m)$

من هذه الحالة ننتج أن رتبة a المقاس m يمكن

أن تكون تقسم $\phi(m)$ (نفسه $\phi(m)$ هو العدد الأولي

الذي يليه m)

مثال إذا أردنا أن نجد ord_2
13

ord_2
13

$$\phi(13) = 12$$

نوجد قدر $2^x \equiv 1 \pmod{13}$ حيث $x \in \{1, 2, 3, 4, 6, 12\}$
نحفظ نوجد هو عدد منته للعدد 12

$$2^2 \equiv 4 \pmod{13}$$

$$2^3 \equiv 8 \pmod{13}$$

$$2^4 \equiv 3 \pmod{13}$$

$$2^6 \equiv 2^4 \cdot 2^2 \equiv 3 \cdot 2^2 \pmod{13}$$

$$\equiv 12 \pmod{13}$$

نعود إلى مثال
بالقائمة

$$2^{12} \equiv 1 \pmod{13} \Rightarrow \text{ord}_2 = 12$$

يقال أن العدد 2 له أولي (أول) للعدد 13

ويشكل عام

- نقول أن العدد a له أولي بالعدد m إذا
و فقط إذا كان

$$\text{ord}_m a = \phi(m)$$

بمعنى آخر إذا كانت $\text{ord}_m a = k$ فإن

$$a^T \equiv a^S \pmod{m}$$

$$T \equiv S \pmod{k}$$

إذا و فقط إذا

البرهان، نفرض ان $a^t \equiv a^s \pmod{m}$ ونفرض ان $t > s$
 عارضا ان $d(a, m) = 1$ فيكون الاختصار على a^s ويكون
 $a^{t-s} \equiv 1 \pmod{m}$

مع البرهان الذي $t-s$ $k \mid (t-s)$ $\Leftrightarrow k \mid t-s$

(مع حقيقة تالية نفرض ان $t \equiv s \pmod{k}$)

نفرض ان $t > s$ مع فترتنا على الترتيب

$$t = k \cdot q + s$$

$$a^t = (a^k)^q \cdot a^s$$

$$\equiv (1)^q \cdot a^s \pmod{m} \equiv a^s \pmod{m}$$

ملاحظة اذ ان k $\text{ord}_m a$ فان الزعداد $a^k, a^{2k}, \dots, a^{(q-1)k}, a^q$ تكون غير متطابقة بالمقاس m

$$\text{ord}_m a^r = \frac{\text{ord}_m a}{d(k, s)} \quad \text{فان} \quad \text{ord}_m a \mid k$$

مبرهنة اذا a عدد اولي للعدد m وكان هذا العدد هو a

$$d(a, m) = \phi(m) \quad \text{اذ} \quad \text{ord}_m a = \phi(m) \quad \text{فان للعدد } m \text{ يوجد}$$

اذا كان p عدد اولي و r هذا اولي للعدد p ان

$$\text{ord}_p r = p-1$$

فان عدد الجذور الأولية لـ p هو $\phi(p-1)$

$$\text{مثال: } p=7 \quad \text{فان } \phi(6)=2 \quad \text{وان} \quad \phi(6)$$

$$1, 2, 3, 6$$

$$\phi(6)=2$$

وبنفس العدد 7 لها جذرا اوليا هما 3 و 5